ATTACKS ON PUBLIC WI-FI TO STEAL VULNERABLE INFORMATION

Jansen Lazaro
University of Manitoba
Department of Computer Science
Research Paper
April 8, 2018

I. ABSTRACT

Wireless communication technologies suffers security weaknesses that can be exploited allowing eavesdroppers to capture data from your mobile devices. In this paper, we will investigate different attacks that is used against unknowing victims who uses public WiFi "hotspots" in places such as transit hubs, airports, and popular social spots like Starbucks and Tim Hortons. More specifically, I will present a brief review of the most used attacks on public WiFi. I will provide them with their description and how each attacks works. Additionally, we will explore how to avoid these attacks to prevent them from happening. This paper will also outline the steps and methods of conducting these attacks.

II. INTRODUCTION

You've heard of a drive-by shooting, but maybe not drive by hacking. It's a worrisome sort of cybercrime in which burglars sit in a car outside your local Starbucks and use laptop computers to hack into your phones and personal computers by snagging data as they travel around your city. That's how hackers could capture important information such as your password and even your credit-card

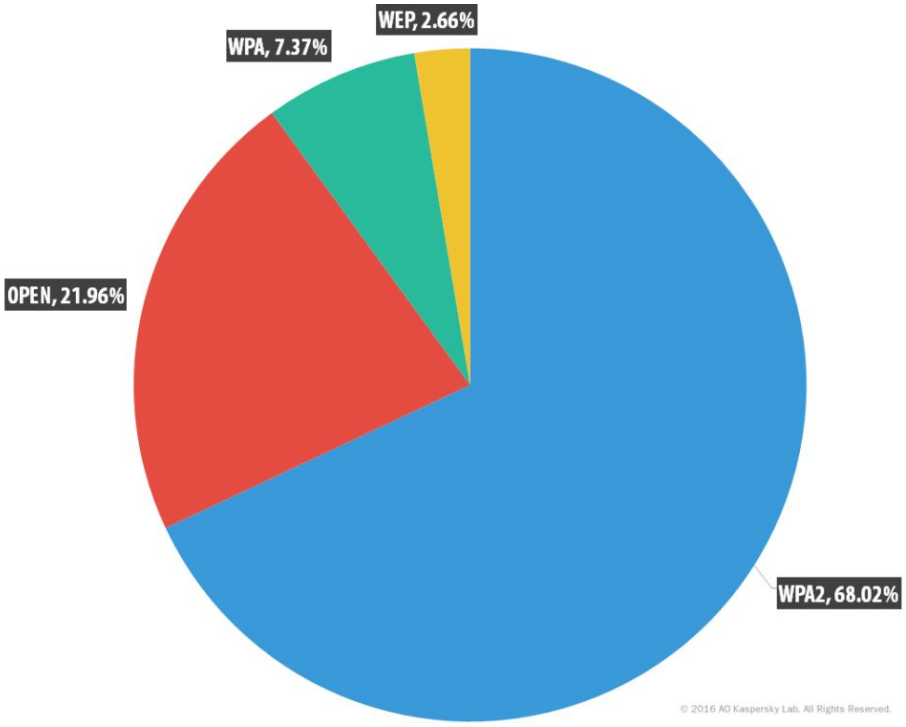
numbers. The very nature of wireless Wi-Fi networks means that hackers or criminals simply need to be located near an access point in order to eavesdrop and intercept network traffic. Poorly configured access point encryption or services that allow data to be sent without any encryption pose a serious threat to user data. Confidential data can be protected by encrypting traffic at wireless access points. In fact, this method of protection is now considered essential for all WiFi networks.

Our current era is driven by technology. The internet has become a part of everyone's lives. We are in an age where everyone is connected. Nowadays, free public WiFi are widely and readily available in larger cities—airports, restaurants, coffee shops, libraries, public transport, hotel rooms, you name it. Of course, we all know jumping on a free Internet connection can be a convenient way to access online accounts, catch up on work, and check emails while on the go. However, the security risks should not be ignored since you could be making yourself an easy target for hackers while putting your information and more at risk. The major hazard with public Wi-Fi is that all the information you're transferring between your computer and the computer that you're accessing is available to everyone on the network.

The purpose of this paper is to explain the security vulnerabilities of WiFi in public places and share some concepts for better understanding attacks that can be used on this network. The attacks we will discuss includes: packet sniffing, rogue access points, arp spoofing, etc. The remaining sections of this paper are organized as follows. Section 3 discusses the security of wireless networks. The different attacks that can be used are discussed in Section 4. Section 5 presents the defense strategies and finally Section 5 concludes the paper.

III. SECURITY

To protect wireless networks, there are various wireless security protocols which include WEP, WPA, and WPA2, each having their own strengths and weaknesses.Wired networks are more secure than wireless networks since wired networks send data between two points, A and B, which are connected by a cable. In a wireless network, data is broadcasted in every direction to every device that happen to be listening.



This image, taken from Kaspersky Lab, is showing that approximately 21.96% of WiFi hotspots in the world do not use any encryption at all. Anyone who has the right device can easily intercept and store all user traffic to use it for their own interest. Fortunately, modern online banking systems and messengers encrypt their data. However, this is the only thing that prevents users of WiFi networks with unencrypted traffic from revealing their passwords and other essential data when using an unsecure access point.

A. Wire Equivalent Privacy

This was the first type of security protocol that was required to necessary to gain access to a local area network. You can use different key sizes here depending on where you are in the world and depending on the type of implementation that you want to use on your network. However, it has been found that this protocol has a very significant vulnerability inside of the mechanisms used to encrypt and decrypt this data over the network. This vulnerability is well known thus this protocol is easily hacked.

B. Wireless Protected Access

WPA was established to eliminate these security issues. A set of mainly 5 different security protocols for connecting computers, laptops, tablets, cellphones, etc. The protocol suite provide connectivity for the WPA devices and software. Not as easily compromised as WEP. However, this was just a short-term workaround for WEP. We needed something that was well vetted and standardized. So they came up with WPA2.

C. Wireless Protected Access version 2

WPA2 uses a AES (Advanced Encryption Standard) cipher which is more secure but requires more CPU cycle. This also used a Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which is a much more secure protocol to use for authenticating and making sure that the data within the packets is exactly where it came from.

Overall, it can be said that today's WPA/WPA2 versions are reasonably, but not absolutely, secure. Specifically, It still allow brute-force and dictionary attacks. There are ready-to-use publicly available tools (aircrack-ng and similar software) for performing such attacks, as well as a large number of manuals.

IV. ATTACKS

A. WiFi Sniffing

In a wireless network, the information/data that's sent from your smartphone or from your laptop to the access point is actually broadcasted in every direction for anybody to collect and to analyze and so therefore that posses many problems but how easy is it to actually collect data and network packets on a public open WiFi system. When you connect to a public open WiFi the connection between your device and the WiFi router, data is not just sent directly in the line of sight of the router and with the right equipment, anybody can pick up all those data packets that are floating around in the air. Such devices can be bought easily online in under 20 dollars. After the packets are captured, tools like driftnet and wireshark can be used to examine all of the data and see what's there. You will be able to see what websites people have been visiting and you'll also be able to grab any picture that have been flowing around in the air to see what people have been viewing.

B. Rogue Hotspots

Grabbing things out of the air is one thing that can happen on a WiFi hotspot but

it is not the only thing that can be exploited. Another problem can be is people can set up rogue access points/fake access points deliberately just to lure you in so that you connect to them and then they have control over you traffic. For example, maybe you are in a particular coffee shop and it doesn't have WiFi and then one day you see that it does. You connect to this network without your knowledge that this is a rogue access point. Everything that you send over the internet goes to the eavesdropper laptop first where he can store it and he can also manipulate it and worst of all he can redirect it so you think you are going to facebook.com but in fact what comes up is a website that looks very similar if not a clone of facebook.com but in reality it's a fake website that the eavesdropper put up deliberately just to capture your login credentials.

C. Spoofing

Another thing that can happen when you connect to a public WiFi is a thing called arp spoofing. Every single device that has a network card in the world has a thing called a MAC address which stands for media access control address and it's unique. They're established in the factory when it goes out of the door and everyone in the world is different whether it's a PC, or a laptop, or a phone they've all got network adapter that has unique addresses on them. This is used on to identify which devices requested/sent data over a network. When you're in an public WiFi, hackers can spoof that by saying they own your address and that means now traffic comes to the hacker where he can do lots of different things like phishing attack, man-in-the-middle attacks, etc

.

D. Man-in-the-Middle Attack

This is an attack technique that is like WiFi sniffing we previously discussed where the attacker is able to watch exactly what's going on between two communicating system. The attacker can capture packets, inject his own information, change information or just simply watch what's going on without anyone noticing it. The attacker acts as an intermediary and the network traffic is routed through the attacking device. This state of unauthorized and intentionally changed network topology enables the attacker to eavesdrop on passed communication.

V. DEFENSE STRATEGIES

There are several simple rules to fight avoid these attacks. The damage is less when you know your vulnerabilities. To help protect personal data when using open WiFi networks, follow these rules:

- When you really need to use a public WiFi, connect via a Virtual Private Network. With a VPN, encrypted traffic is transmitted over a protected tunnel. This will make your data unreadable to criminals.
- Always keep you system up to date to prevent intruders to exploit known bugs in outdated software/system.
- Do not trust networks that are not password-protected
- Avoid being target for cyber criminals by enabling the "Always use a secure connection" option in your device settings.

- Turn off your WiFi connection when you are not using it.
- Refrain from entering your login details in public wifi and absolutely do not perform any banking operations or enter your card details anywhere. Limit yourself to basic user actions.
- Always check the app permissions before installing.
- Turn off Bluetooth on your devices when not in use or just don't use them at all in public places.

There is no real protection that can completely prevent attackers from exploiting your connection over a public WiFi but these things can be done to make it harder for the attackers.

VI. CONCLUSION

The field of computer security is becoming more challenging everyday not only for companies but also for an average user. There is more chance of you getting hacked than getting mugged. If you plan on using public Wi-Fi, make sure that you're connecting to the right network and don't access anything sensitive, like your bank account. It's simply not worth the risk. This paper detailed wireless network security and discusses the dangers of using unsecured public WiFi.

REFERENCES

Matthew Denis, Carlos Zena, Thaier Hayajneh (2016). Penetration Testing: Concepts, Attack Methods, and Defense Strategies.
https://ieeexplore-ieee-org.uml.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=7494156
Kerner Sm, Bio VF (2013). eWEEK. WiFi Pineapple Penetration-Testing Tool Sparks Interest at DEF CON
https://www.eweek.com/security/wifi-pineapple-penetration-testing-tool-sparks-interest-at-def-con
Martin Vondracek, Jan Pluskal, Ondrej Rysavy (2018). "Automated Man-in-the-Middle Attack Against Wi‑Fi Networks," Journal of Digital Forensics, Security and Law: Vol. 13 : No. 1 , Article 9. DOI: https://doi.org/10.15394/jdfsl.2018.1495
https://commons.erau.edu/cgi/viewcontent.cgi?article=1495&context=jdfsl
Sidharth Shekhar (June 2016). Beware! Here's How Public Wi-Fi is Used to Steal Information
https://www.pcquest.com/why-uisng-public-wi-fi-can-be-dangerous/
Gary Sims (February 2018). How easy is it to capture data on public free Wi-Fi?
https://www.androidauthority.com/capture-data-open-wi-fi-726356/
Denis Legezo (November 2016). Research on unsecured Wi-Fi networks across the world
https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/